(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
10 juillet 2003 (10.07.2003)

PCT

(10) Numéro de publication internationale
WO 2003/056750 A3

(51) Classification internationale des brevets[7] : H04L 9/32

(21) Numéro de la demande internationale :
PCT/FR2002/004502

(22) Date de dépôt international :
20 décembre 2002 (20.12.2002)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
01/16950 27 décembre 2001 (27.12.2001) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **FRANCE TELECOM** [FR/FR]; 6, place d'Alleray, F-75015 Paris (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **VARDITTI MODIANO, David** [FR/FR]; 46ter, rue Paul Vaillant-couturier, F-92140 Clamart (FR). **CANARD, Sébastien** [FR/FR]; 4, résidence Olympia, F-14000 Caen (FR). **GIRAULT, Marc** [FR/FR]; 4, rue Viviane, F-14000 Caen (FR). **TRAORE, Jacques** [FR/FR]; 14, rue Emile Dron, F-81100 Flers (FR).

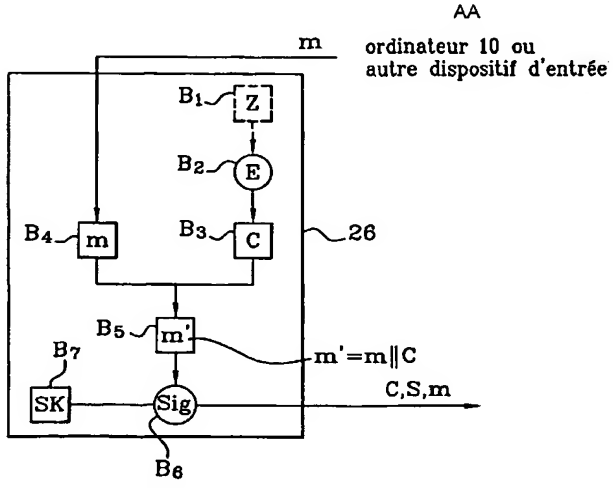
(74) Mandataires : **SOMNIER, Jean-Louis** etc.; Cabinet Ballot, 122, rue Edouard Vaillant, F-92593 Levallois-Perret Cedex (FR).

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG,

[Suite sur la page suivante]

(54) Title: CRYPTOGRAPHIC SYSTEM FOR GROUP SIGNATURE

(54) Titre : SYSTEME CRYPTOGRAPHIQUE DE SIGNATURE DE GROUPE



AA...COMPUTER 10 OR OTHER INPUT DEVICE

(57) Abstract: The invention concerns a system enabling a member (M) of a group (G) to produce, by means of customized data (z; K), a message (m) accompanied by a signature (8) proving to a verifier that the message originates from a member of the group (G). The invention is characterized in that the customized data is in the form of an electronic physical medium (26). Advantageously, the latter also incorporates: encrypting means (B3) for producing a customized cipher (C) from the customized data prior to the signature S of the message (m), means (B5) for producing a combination of a message m to be signed and the cipher (C) associated with said message, for example in the form of a concatenation of the message (m) with the cipher (C), and means (B6) for signing (Sig) the message (m) with the customized data (z; K) in the form of a cipher (C) associated with said message. Advantageously, the physical medium is a smart card (26) or the like.

[Suite sur la page suivante]

WO 2003/056750 A3

SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) **États désignés** *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclaration en vertu de la règle 4.17 :

— *relative à la qualité d'inventeur (règle 4.17.iv)) pour US seulement*

Publiée :

— *avec rapport de recherche internationale*

(88) **Date de publication du rapport de recherche internationale:** 26 février 2004

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) **Abrégé :** Le système permet à un membre (M) d'un groupe (G) de produire, à l'aide d'une donnée personnalisée (z ; K), un message (m) accompagné d'une signature (S) prouvant à un vérifieur que le message provient d'un membre du groupe (G), et se caractérise par le fait que la donnée personnalisée se présente sous forme intégrée à un support matériel électronique (26). Ce dernier intègre avantageusement aussi : des moyens (B3) de chiffrement pour réaliser un chiffré (C) personnalisé à partir de la donnée personnalisée préalablement à la signature S du message (m), des moyens (B5) pour réaliser une combinaison d'un message m à signer et le chiffré C associé à ce message, par exemple sous forme de concaténation du message m avec le chiffré (C), et des moyens (B6) de signature (Sig) du message (m) avec la donnée personnalisée (z ; K) sous forme de chiffré (C) associé à ce messge. Avantageusement, le support matériel est une carte à puce (26) ou analogue.

INTERNATIONAL SEARCH REPORT

Interna[redacted] Application No
PCT/FR [redacted]04502

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CAMENISCH J ET AL: "EFFICIENT GROUP SIGNATURE SCHEMES FOR LARGE GROUPS" ADVANCES IN CRYPTOLOGY - CRYPTO '97. SANTA BARBARA, AUG. 17 - 21, 1997, PROCEEDINGS OF THE ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE (CRYPTO), BERLIN, SPRINGER, DE, vol. CONF. 17, 17 August 1997 (1997-08-17), pages 410-424, XP000767547 ISBN: 3-540-63384-7 cited in the application abstract page 411, line 10 -page 413, line 9 page 416, line 16 -page 423, line 15 --- -/--	1,15-17

[X] Further documents are listed in the continuation of box C.

[ ] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
4 June 2003	16/06/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Dujardin, C

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	ATENIESE G ET AL: "A PRACTICAL AND PROVABLY SECURE COALITION-RESISTANT GROUP SIGNATURESCHEME" ADVANCES IN CRYPTOLOGY. CRYPTO 2000. 20TH ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE, SANTA BARBARA, CA, AUG. 20 - 24, 2000. PROCEEDINGS, LECTURE NOTES IN COMPUTER SCIENCE;VOL. 1880, BERLIN: SPRINGER, DE, 20 August 2000 (2000-08-20), pages 255-270, XP001003407 ISBN: 3-540-67907-3 cited in the application abstract page 261, line 14 -page 265, line 13	1,15-17
A	CHAUM D: "GROUP SIGNATURES" ADVANCES IN CRYPTOLOGY- EUROCRYPT. INTERNATIONAL CONFERENCE ON THE THEORY AND APPLICATION OF CRYPTOGRAPHIC TECHNIQUES, SPRINGER VERLAG, DE, April 1991 (1991-04), pages 257-265, XP000900793 the whole document	1,15-17
A	BONETTI P ET AL: "The Italian academic community's electronic voting system" COMPUTER NETWORKS, ELSEVIER SCIENCE PUBLISHERS B.V., AMSTERDAM, NL, vol. 34, no. 6, December 2000 (2000-12), pages 851-860, XP004304824 ISSN: 1389-1286 page 852, right-hand column, line 3 - line 5 page 853, left-hand column, line 14 - line 17 page 855, right-hand column, line 8 -page 859, right-hand column, line 7; table 1	1,13,14, 18

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR [redacted]4502

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L9/32

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	CAMENISCH J ET AL: "EFFICIENT GROUP SIGNATURE SCHEMES FOR LARGE GROUPS" ADVANCES IN CRYPTOLOGY - CRYPTO '97. SANTA BARBARA, AUG. 17 - 21, 1997, PROCEEDINGS OF THE ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE (CRYPTO), BERLIN, SPRINGER, DE, vol. CONF. 17, 17 août 1997 (1997-08-17), pages 410-424, XP000767547 ISBN: 3-540-63384-7 cité dans la demande abrégé page 411, ligne 10 -page 413, ligne 9 page 416, ligne 16 -page 423, ligne 15 --- -/--	1,15-17

[X] Voir la suite du cadre C pour la fin de la liste des documents

[ ] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
4 juin 2003	16/06/2003

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Dujardin, C

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR [redacted]04502

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
A	ATENIESE G ET AL: "A PRACTICAL AND PROVABLY SECURE COALITION-RESISTANT GROUP SIGNATURESCHEME" ADVANCES IN CRYPTOLOGY. CRYPTO 2000. 20TH ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE, SANTA BARBARA, CA, AUG. 20 - 24, 2000. PROCEEDINGS, LECTURE NOTES IN COMPUTER SCIENCE;VOL. 1880, BERLIN: SPRINGER, DE, 20 août 2000 (2000-08-20), pages 255-270, XP001003407 ISBN: 3-540-67907-3 cité dans la demande abrégé page 261, ligne 14 -page 265, ligne 13 ---	1,15-17
A	CHAUM D: "GROUP SIGNATURES" ADVANCES IN CRYPTOLOGY- EUROCRYPT. INTERNATIONAL CONFERENCE ON THE THEORY AND APPLICATION OF CRYPTOGRAPHIC TECHNIQUES, SPRINGER VERLAG, DE, avril 1991 (1991-04), pages 257-265, XP000900793 le document en entier ---	1,15-17
A	BONETTI P ET AL: "The Italian academic community's electronic voting system" COMPUTER NETWORKS, ELSEVIER SCIENCE PUBLISHERS B.V., AMSTERDAM, NL, vol. 34, no. 6, décembre 2000 (2000-12), pages 851-860, XP004304824 ISSN: 1389-1286 page 852, colonne de droite, ligne 3 - ligne 5 page 853, colonne de gauche, ligne 14 - ligne 17 page 855, colonne de droite, ligne 8 -page 859, colonne de droite, ligne 7; tableau 1 -----	1,13,14, 18